Research Article

Three-key 12-note polyhybrid encryption

Cemil KARAÇAM*[1] Eralp AKAY [2] Ilgaz ÜNAL[3]

[1]**Corresponding Author, Muğla Art and Science Center, Departmant of Mathematics,*
cemil-karacam@hotmail.com, Orcid.org 0000-0001-7186-5114
[2] *Muğla Art and Science Center, Departmant of Mathematics,*
eralpakay2009@gmail.com., *Orcid.org* 0009-0006-6704-7323
[3] *Muğla Art and Scince Center, Departman of Mathematics,*
gazun2009@mail.com *Orcid.org* 0009-0005-8994-8846

Abstract

In this paper, a dynamic encryption algorithm rich in music and mathematics has been developed. The foundation of this algorithm is the Pythagorean diatonic note series, combined with the alteration tools (Accidentals) in Turkish music. A 12-note, three-key system with equivalent notes we defined was used to create three different and two-notation encryption databases. The corresponding values of characters' ASCII codes in base 12 were structured to match the 12-tone note system in accordance with three different key structures. Formulas necessary for the integration of the three-key system were derived. From a transmission perspective, a symmetric encryption algorithm supporting addition, subtraction, and symmetry opearations in base 12 was created. Fixed and dynamic parameter versions of the encryption key were designed. A musical composite function operation, based on the infrastructure of flat, sharp, and the 12-tone note system, was designed and implemented, benefiting from the properties of flat and sharp accidentals. A dynamic musical encryption design was developed with time and serial numbers, three different musical keys, and a staff-supported mathematical composite function structure, ensuring data transmission and character set. Through the integration of mathematical operations with musical terms, an original algorithm was designed, making it highly secure against cryptographic attacks,*while* reducing character similarity. *In terms of data diversity, mathematical operations, and transmission variety, it stands out from similar studies due to its richness.*

Keywords: *Musical encryption, Musical keys, Dynamic encryption, 12-tone note system*
MSC: 94A60,68Q25,51N99, 52C25

Received: 06/12/2024
Accepted: 16/12/2024

1. INTRODUCTION

Encryption is a critical method used to protect information by converting data into an unreadable format, ensuring that only authorized individuals can access the original message. The scientific principles behind encryption involve complex mathematical concepts, including prime numbers, number sequences, modular arithmetic, matrices, and various algebraic and geometric structures (Stallings, 2017). Music, with its mathematical foundations, has also found its place in encryption research, offering innovative approaches for securing data through musical transformations. These approaches utilize the rich structure of musical elements such as notes, rhythms, and scales to encode and decode information.

Several studies have investigated.the intersection of music and mathematics in the context of encryption. For instance, Bakım (2014) investigated the relationship between the Fibonacci sequence, the golden ratio, and music in his master's thesis, illustrating how these mathematical concepts can be applied to musical composition. Similarly, Erol and Tavit (2018) examined the use of Pascal's Triangle in music cryptology, utilizing its numerical properties to create encryption systems based on musical notes. More recently, Algül and Tavit (2021) proposed an encryption system that varies based on both time and location, using Fibonacci and Lucas number sequences to encode musical notes. Other research, such as the work by Denizkuşu (2023), has further expanded encryption methods by incorporating accidentals (sharp and flat notes), providing a more nuanced approach to musical cryptography.

Despite these advances, a gap in the literature remains in the development of a 12-note dynamic encryption system that integrates mathematical principles with fundamental musical concepts such as the "do", "sol", and "fa" notes. These notes, central to Western music theory, are promising key elements in an encryption algorithm. This research seeks to address this gap by proposing a novel encryption framework based on the 12-tone system, drawing upon mathematical constructs such as modular arithmetic and number sequences to enhance security and complexity. By doing so, this study aims to contribute to the growing body of interdisciplinary research in music and cryptography.

2. MATERIALS and METHODS

The project is a mathematical modeling study. In this modeling, the classical 7-note system is transformed into the 12-note system through the concept of equivalent notes.

Before our modeling work, a literature review was conducted to examine studies close to our area of research.

In our study, a dynamic encryption algorithm based on various musical concepts will be designed.. These concepts are briefly explained as follows

- **Staff**: A staff, or stave, is a structure consisting of 4 equal intervals and 5 parallel lines on which notes are placed, along with accidentals (sharp or flat) and rhythm values.

Figure 1: Staff

- **Clef**: A key or clef is a sign placed at the beginning of the staff in music, and it determines the names of the notes according to the line it is placed on.

In the classical notation system, clefs are arranged in a 7-note sequence. For example, the **C clef** is {C, D, E, F, G, A, B}. Let us provide the note sequences for the clefs:

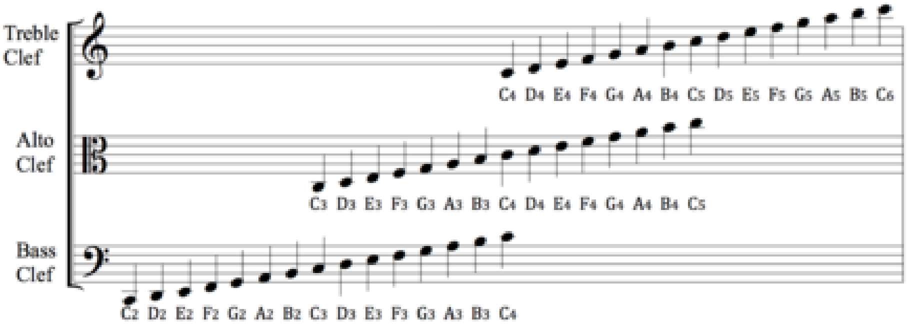
Treble Clef
C4 D4 E4 F4 G4 A4 B4 C5 D5 E5 F5 G5 A5 B5 C6
Alto Clef
C3 D3 E3 F3 G3 A3 B3 C4 D4 E4 F4 G4 A4 B4 C5
Bass Clef
C2 D2 E2 F2 G2 A2 B2 C3 D3 E3 F3 G3 A3 B3 C4

Figure 2: Clefs with Notes

Do	Re	Mi	Fa	Sol	La	Si
C	D	E	F	G	A	B

Table 1: The Letter Representations of the Notes

- **Flat (♭)**: An accidental that lowers the pitch of the note by a half-step.

- **Sharp (♯)**: An accidental that raises the pitch of the note by a half-step.

Let us provide the relationship between flat and sharp for two consecutive notes, denoted as **x** and **y**.

$$\boxed{x} \longrightarrow \boxed{x^{b}} = \boxed{y^{\#}} \longleftarrow \boxed{y}$$

Figure 3: Reolitonship Between Flat and Sarp

All equivalent notes:

$C^{\#} \equiv$	D^{b}
$D^{\#} \equiv$	E^{b}
$E \equiv$	F^{b}
$F^{\#} \equiv$	G^{b}
$G^{\#} \equiv$	A^{b}
$A^{\#} \equiv$	B^{b}

$$\longrightarrow \boxed{E^{\#} \equiv F}$$

Since there is a half-step between **E** and **F**, the sharp of **E** is equivalent to **F**.

Table 2: Equivalent Notes

The notes are arranged differently according to different clefs. When a sequence number is assigned to the notes according to this arrangement, the following tables are formed:

C	$C^{\#}$	D	$D^{\#}$	E	F	$F^{\#}$	G	$G^{\#}$	A	$A^{\#}$	B
0	1	2	3	4	5	6	7	8	9	10	11

Table 3: Sequence Numbers of the Notes According to the C Clef

G	$G^{\#}$	A	$A^{\#}$	B	C	$C^{\#}$	D	$D^{\#}$	E	F	$F^{\#}$
0	1	2	3	4	5	6	7	8	9	10	11

Table 4: Sequence Numbers of the Notes According to the G Clef

F	F#	G	G#	A	A#	B	C	C#	D	D#	E
0	1	2	3	4	5	6	7	8	9	10	11

Table 5: Sequence Numbers of the Notes According to the F Clef

3. RESULTS

3.1. Encryption

The encryption algorithm is provided below.

1. Our data set consists of a total of 96 items, divided into 4 main groups.

Charater	Big Letters	Litle Letters	Numbers	Symbols
Unit	32	32	10	24

Table 6: Dataset

2. The key we want to use is selected. The numerical values of the notes in this clef are used.

Figure 4: Clefs (from right to left G clef, F clef, C clef)

3. Separate data sets will be created for each of the three clefs.
4. A transformation algorithm between the three clefs will be created.
5. The ASCII codes of the characters are converted to base 12, and the digits of the resulting number are matched with the notes in the corresponding key.
6. If the number obtained from the transformation is three digits long, the last digit will be shown in parentheses, ensuring that the characters maintain an equal digit structure, which will facilitate decryption.
7. Two different versions of the transformation notes will be created, following the equivalent note algorithm in point 5.

3.1.1 Types of Transmission

- Encryption and decryption of data according to the note transformation algorithm.
- Two different clef-based encryptions will be designed in base 12.
- Encryption using the $\oplus$ and $\ominus$ subtraction operations with keys.
- Text encryption using key symmetry operations.
- Encryption using the concept of a staff in music, along with clef, flat, and sharp accidentals.
- Dynamic encryption through mathematical composite operations.
- Dynamic encryption based on date and name for clef selection.

3.1.1.1Key Transformations

The following algorithm has been designed for transformations between clefs. In this algorithm, the operation expressed in each section is the transformation of the numerical value of the note in one key to the next key. 1. Transformation rule from the 1st key to the 2nd key: "y = x + a (mod 12)" is defined.

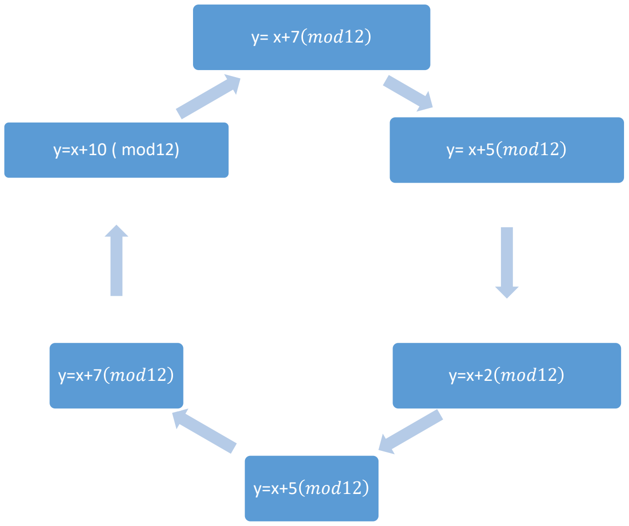

Figure 5: Moduler Clef Transmission

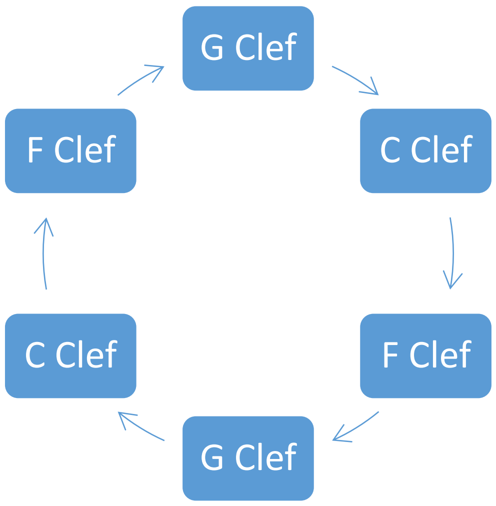

Figure 6: Clef Transmission

	C	C$^{\#}$	D	D$^{\#}$	E	F	F$^{\#}$	G	G$^{\#}$	A	A$^{\#}$	B
C Clef	0	1	2	3	4	5	6	7	8	9	10	11
F Clef	7	8	9	10	11	0	1	2	3	4	5	6
G Clef	5	6	7	8	9	10	11	0	1	2	3	4

Table 7: Table of Key Transformations

For example, let's perform a transformation from the **C** clef to the **F** clef.

Let **x** be the numerical value of any note in the **C** clef, and **y** be the value of this note in the **F** clef.

Our transformation operation is defined as: y = x + 7 (mod 12)

When D$^{\#}$ = 3, the transformation y = 3 + 7 (mod 12) → "y = 10 = D$^{\#}$ will occur.

3.1.1.2 Transformation of the Data Set

A clef is selected. The ASCII code of each character is converted to base 12, then transformed into a note using the 12-note system, and subsequently, some notes are replaced with their equivalent notes. The goal here is to prevent decryption against the sequential order derived from the ASCII code structure.

For example, in the **C** clef, the ASCII code of the character **A** is 65.

65 = $(55)_{12}$ = **F-F** is converted into the note system. Due to the equivalent note structure, **F-F** has various representations such as **E$^{\#}$-E$^{\#}$**, **E$^{\#}$-F**, **F-E$^{\#}$**, and so on.

Order	Character	ASCII Code	12 Base Value	Note Sequence	Equivalent Note
0	A	65	55	FF	$E^{\#}E^{\#}$
1	B	66	56	$FF^{\#}$	$E^{\#}G^{b}$
2	C	67	57	FG	$E^{\#}G$
3	Ç	128	(10)8	$A^{\#}G^{\#}$	$B^{b}A^{b}$
4	D	68	58	$FG^{\#}$	$E^{\#}A^{b}$
5	E	69	59	FA	$E^{\#}A$
6	F	70	5(10)	$FA^{\#}$	$E^{\#}B^{b}$
7	G	71	5(11)	FB	$E^{\#}C^{b}$
8	Ğ	258	1(9)6	$C^{\#}AF^{\#}$	$D^{b}AG^{b}$
9	H	72	60	$F^{\#}C$	$G^{b}B^{\#}$
10	I	73	61	$F^{\#}C^{\#}$	$G^{b}D^{b}$
11	İ	214	15(10)	$C^{\#}FB^{\#}$	$D^{b}E^{\#}B^{b}$
12	J	74	62	$F^{\#}D$	$G^{b}D$
13	K	75	63	$F^{\#}D^{\#}$	$G^{b}E^{b}$
14	L	76	64	$F^{\#}E$	$G^{b}F^{b}$
15	M	77	65	$F^{\#}F$	$G^{b}E^{\#}$
16	N	78	66	$F^{\#}F^{\#}$	$G^{b}\ G^{b}$
17	O	79	67	$F^{\#}G$	$G^{b}G$
18	Ö	153	1(0)9	$C^{\#}CA$	$D^{b}B^{\#}A$
19	P	80	68	$F^{\#}G^{\#}$	$G^{b}A^{b}$
20	Q	81	69	$F^{\#}A$	$G^{b}A$
21	R	82	6(10)	$F^{\#}A^{\#}$	$G^{b}B^{b}$
22	S	83	6(11)	$F^{\#}B$	$G^{b}C^{b}$
23	Ş	261	1(9)9	$C^{\#}AA$	$D^{b}AA$
24	T	84	70	GC	$GB^{\#}$
25	U	85	71	$GC^{\#}$	GD^{b}
26	Ü	154	10(10)	$C^{\#}CA^{\#}$	$D^{b}B^{\#}B^{b}$
27	V	86	72	GD	GD
28	W	87	73	$GD^{\#}$	GE^{b}
29	X	88	74	GE	GF^{b}
30	Y	89	75	GF	$GE^{\#}$
31	Z	90	76	$GF^{\#}$	GG^{b}

Order	Character	ASCII Code	12 Base Value	Nota Sequence	Equivalent Note
0	a	97	81	$G^{\#}C^{\#}$	$A^{b}D^{b}$
1	b	98	82	$G^{\#}D$	$A^{b}D$
2	c	99	83	$G^{\#}D^{\#}$	$A^{b}E^{b}$
3	ç	135	(11)3	$BD^{\#}$	$C^{b}E^{b}$
4	d	100	84	$G^{\#}E$	$A^{b}F^{b}$
5	e	101	85	$G^{\#}F$	$A^{b}E^{\#}$
6	f	102	86	$G^{\#}F^{\#}$	$A^{b}G^{b}$
7	g	103	87	$G^{\#}G$	$A^{b}G$
8	ğ	259	1(9)7	$C^{\#}AG$	$D^{b}AG$
9	h	104	88	$G^{\#}G^{\#}$	$A^{b}A^{b}$
10	ı	213	1(5)9	$C^{\#}FA$	$D^{b}E^{\#}A$
11	i	105	89	$G^{\#}A$	$A^{b}A$
12	j	106	8(10)	$G^{\#}A^{\#}$	$A^{b}B^{b}$
13	k	107	8(11)	$G^{\#}B$	$A^{b}C^{b}$
14	l	108	90	AC	$AB^{\#}$
15	m	109	91	$AC^{\#}$	AD^{b}
16	n	110	92	AD	AD
17	o	111	93	$AD^{\#}$	AE^{b}
18	ö	148	1(0)4	$C^{\#}CE$	$D^{b}B^{\#}F^{b}$
19	p	112	94	AE	AF^{b}
20	q	113	95	AF	$AE^{\#}$
21	r	114	96	$AF^{\#}$	AG^{b}
22	s	115	97	AG	AG
23	ş	260	1(9)8	$C^{\#}AG^{\#}$	$D^{b}AA^{b}$
24	t	116	98	$AG^{\#}$	AA^{b}
25	u	117	99	AA	AA
26	ü	125	(10)5	$A^{\#}F$	$B^{b}E^{\#}$
27	v	118	9(10)	$AA^{\#}$	AB^{b}
28	w	119	9(11)	AB	AC^{b}
29	x	120	(10)0	$A^{\#}C$	$B^{b}B^{\#}$
30	y	121	(10)1	$A^{\#}C^{\#}$	$B^{b}D^{b}$
31	z	122	(10)2	$B^{\#}D$	$B^{b}D$

Table 7: Uppercases Transmission According to C Clef **Table 8:** Lowercases Transmission According to C Clef

Order	Character	ASCII Code	12 Base Value	Note Sequence	Eqivalent Note
0	(space)	32	28	DG$^{\#}$	DA^{b}
1	!	33	29	DA	DA
2	#	35	2(11)	DB	DC^{b}
3	$	36	30	D$^{\#}$C	E^{b}B$^{\#}$
4	‘	39	33	D$^{\#}$D$^{\#}$	E^{b}E^{b}
5	(	40	34	D$^{\#}$E	E^{b}F^{b}
6	)	41	35	D$^{\#}$F	E^{b}E$^{\#}$
7	*	42	36	D$^{\#}$F$^{\#}$	E^{b}G^{b}
8	+	43	37	D$^{\#}$G	E^{b}G
9	,	44	38	D$^{\#}$G$^{\#}$	E^{b}A^{b}
10	-	45	39	D$^{\#}$A	E^{b}A
11	.	46	3(10)	D$^{\#}$A$^{\#}$	E^{b}B^{b}
12	/	47	3(11)	D$^{\#}$B	E^{b}C^{b}
13	:	58	4(10)	EA$^{\#}$	A^{b}B^{b}
14	<	60	50	FC	E$^{\#}$B$^{\#}$
15	=	61	51	FC$^{\#}$	E$^{\#}$D^{b}
16	>	62	52	FD	E$^{\#}$D
17	?	63	53	FD$^{\#}$	E$^{\#}$E^{b}
18	@	64	54	FE	E$^{\#}$F^{b}
19	[	91	77	GG	GG
20	\	92	78	GG$^{\#}$	GA^{b}
21	]	93	79	GA	GA
22	–	95	7(11)	GB	GC^{b}
23	≥	256	1(9)4	C$^{\#}$AE	D^{b}AF^{b}
24	≤	257	1(9)5	C$^{\#}$AF	D^{b}AE$^{\#}$

Order	Character	ASCII Code	12 B.Value	Note S.	E Note
0	0	48	40	EC	F^{b}Si$^{\#}$
1	1	49	41	EC$^{\#}$	F^{b}D^{b}
2	2	50	42	ED	F^{b}D
3	3	51	43	ED$^{\#}$	F^{b}E^{b}
4	4	52	44	EE	F^{b}F^{b}
5	5	53	45	EF	F^{b}E$^{\#}$
6	6	54	46	EF$^{\#}$	F^{b}G^{b}
7	7	55	47	EG	F^{b}G
8	8	56	48	EG$^{\#}$	F^{b}A^{b}
9	9	57	49	EA	F^{b}A

Table 10: Numbers Transmission According to C Clef

Order	Character	ASCII Code	12 Base Value	Note Sequence	Equivalent Note
0	A	65	55	A$^{\#}$A$^{\#}$	B^{b}B^{b}
1	B	66	56	A$^{\#}$B	B^{b}B
2	C	67	57	A$^{\#}$C	B^{b}C

Order	Character	ASCII Code	12 Base Value	Nota Sequence	Equivalent Note
0	a	97	81	C$^{\#}$F$^{\#}$	D^{b}G^{b}
1	b	98	82	C$^{\#}$G	D^{b}G
2	c	99	83	C$^{\#}$G$^{\#}$	D^{b}A^{b}
3	ç	135	(11)3	EG$^{\#}$	F^{b}A^{b}
4	d	100	84	C$^{\#}$A	D^{b}A
5	e	101	85	C$^{\#}$A$^{\#}$	D^{b}B^{b}
6	f	102	86	C$^{\#}$B	D^{b}B
7	g	103	87	C$^{\#}$C	D^{b}C
8	ğ	259	1(9)7	F$^{\#}$DC	G^{b}DC
9	h	104	88	C$^{\#}$C$^{\#}$	D^{b}D^{b}
10	ı	213	1(5)9	F$^{\#}$A$^{\#}$D	G^{b}B^{b}D
11	i	105	89	C$^{\#}$D	D^{b}D
12	j	106	8(10)	C$^{\#}$D$^{\#}$	D^{b}E^{b}
13	k	107	8(11)	C$^{\#}$E	D^{b}F^{b}
14	l	108	90	DF	DE$^{\#}$
15	m	109	91	DF$^{\#}$	DG^{b}
16	n	110	92	DG	DG
17	o	111	93	DG$^{\#}$	DA^{b}
18	ö	148	1(0)4	F$^{\#}$FA	G^{b}FA
19	p	112	94	DA	DA
20	q	113	95	DA$^{\#}$	DB^{b}
21	r	114	96	DB	DB
22	s	115	97	DC	DC
23	ş	260	1(9)8	F$^{\#}$DC$^{\#}$	G^{b}DD^{b}
24	t	116	98	DC$^{\#}$	DD^{b}
25	u	117	99	DD	DD
26	ü	125	(10)5	D$^{\#}$A$^{\#}$	E^{b}B^{b}
27	v	118	9(10)	DD$^{\#}$	DE^{b}
28	w	119	9(11)	DE	DF^{b}
29	x	120	(10)0	D$^{\#}$F	E^{b}E$^{\#}$
30	y	121	(10)1	D$^{\#}$F$^{\#}$	E^{b}G^{b}
31	z	122	(10)2	D$^{\#}$G	E^{b}G

3	Ç	128	(10)8	$D^{\#}C^{\#}$	$E^{b}D^{b}$
4	D	68	58	$A^{\#}C^{\#}$	$B^{b}D^{b}$
5	E	69	59	$A^{\#}D$	$B^{b}D$
6	F	70	5(10)	$A^{\#}D^{\#}$	$B^{b}E^{b}$
7	G	71	5(11)	$A^{\#}E$	$B^{b}F^{b}$
8	Ğ	258	1(9)6	$F^{\#}DB$	$G^{b}DB$
9	H	72	60	BF	BF
10	I	73	61	$BF^{\#}$	BG^{b}
11	İ	214	15(10)	$D^{\#}FA^{\#}$	$E^{b}G^{b}B^{b}$
12	J	74	62	BG	BG
13	K	75	63	$BG^{\#}$	BA^{b}
14	L	76	64	BA	BA
15	M	77	65	$BA^{\#}$	BB^{b}
16	N	78	66	BB	BB
17	O	79	67	BC	BC
18	Ö	153	1(0)9	$F^{\#}FD$	$G^{b}FD$
19	P	80	68	$BC^{\#}$	BD^{b}
20	Q	81	69	BD	BD
21	R	82	6(10)	$BD^{\#}$	BE^{b}
22	S	83	6(11)	BE	BF^{b}
23	Ş	261	1(9)9	$F^{\#}DD$	$G^{b}RR$
24	T	84	70	CF	$CE^{\#}$
25	U	85	71	$CF^{\#}$	CG^{b}
26	Ü	154	10(10)	$D^{\#}D^{\#}$	$E^{b}E^{b}$
27	V	86	72	CG	CG
28	W	87	73	$CG^{\#}$	CA^{b}
29	X	88	74	CA	CA
30	Y	89	75	$CA^{\#}$	CB^{b}
31	Z	90	76	CB	CB

Table 11: Uppercases Transmission
12: Lowercases Transmission
According to F Clef
According to F Clef

Order	Character	ASCII Code	12 Base Value	Nota Sequence	Eqivalent Note
0	(space)	32	28	$GC^{\#}$	GD^{b}
1	!	33	29	GD	GD
2	#	35	2(11)	DB	DC^{b}
3	$	36	30	$D^{\#}C$	$E^{b}B^{\#}$
4	‘	39	33	$D^{\#}D^{\#}$	$E^{b}E^{b}$
5	(	40	34	$D^{\#}E$	$E^{b}F^{b}$
6	)	41	35	$D^{\#}F$	$E^{b}E^{\#}$
7	*	42	36	$D^{\#}F^{\#}$	$E^{b}G^{b}$
8	+	43	37	$D^{\#}G$	$E^{b}G$
9	,	44	38	$D^{\#}G^{\#}$	$E^{b}A^{b}$
10	-	45	39	$D^{\#}A$	$E^{b}A$
11	.	46	3(10)	$D^{\#}A^{\#}$	$E^{b}B^{b}$
12	/	47	3(11)	$D^{\#}B$	$E^{b}C^{b}$
13	:	58	4(10)	$EA^{\#}$	$A^{b}B^{b}$
14	<	60	50	FC	$E^{\#}B^{\#}$
15	=	61	51	$FC^{\#}$	$E^{\#}D^{b}$
16	>	62	52	FD	$E^{\#}D$
17	?	63	53	$FD^{\#}$	$E^{\#}E^{b}$
18	@	64	54	FE	$E^{\#}F^{b}$
19	[	91	77	GG	GG
20	\	92	78	$GG^{\#}$	GA^{b}
21	]	93	79	GA	GA
22	–	95	7(11)	GB	GC^{b}
23	≥	256	1(9)4	$C^{\#}AE$	$D^{b}AF^{b}$
24	≤	257	1(9)5	$C^{\#}AF$	$D^{b}AE^{\#}$

Table 9: Symbols Transmission According to C Clef

Table

Order	Character	ASCII Code	12 B.Value	Note S.	E Note
0	0	48	40	EC	$F^{b}B^{\#}$
1	1	49	41	$EC^{\#}$	$F^{b}D^{b}$
2	2	50	42	ED	$F^{b}D$
3	3	51	43	$ED^{\#}$	$F^{b}E^{b}$
4	4	52	44	EE	$F^{b}F^{b}$
5	5	53	45	EF	$F^{b}E^{\#}$
6	6	54	46	$EF^{\#}$	$F^{b}G^{b}$
7	7	55	47	EG	$F^{b}G$
8	8	56	48	$EG^{\#}$	$F^{b}A^{b}$
9	9	57	49	EA	$F^{b}A$

Table 14: Numbers Transmission According to F Clef

Order	Character	ASCII Code	12 Base Value	Note Sequence	Equivalent Note
0	A	65	55	$A^{\#}A^{\#}$	$B^{b}B^{b}$
1	B	66	56	$A^{\#}B$	$B^{b}B$

2	C	67	57	A$^\#$C	B^{b}C
3	Ç	128	(10)8	D$^\#$C$^\#$	E^{b}D^b
4	D	68	58	A$^\#$C$^\#$	B^{b}D^b
5	E	69	59	A$^\#$D	B^{b}D
6	F	70	5(10)	A$^\#$D$^\#$	B^{b}E^b
7	G	71	5(11)	A$^\#$E	B^{b}F^b
8	Ğ	258	1(9)6	F$^\#$DB	G^{b}DB
9	H	72	60	BF	BF
10	I	73	61	BF$^\#$	BG^b
11	İ	214	15(10)	D$^\#$FA$^\#$	E^{b}G^{b}B^b
12	J	74	62	BG	BG
13	K	75	63	BG$^\#$	BA^b
14	L	76	64	BA	BA
15	M	77	65	BA$^\#$	BB^b
16	N	78	66	BB	BB
17	O	79	67	BC	BC
18	Ö	153	1(0)9	F$^\#$FD	G^{b}FD
19	P	80	68	BC$^\#$	BD^b
20	Q	81	69	BD	BD
21	R	82	6(10)	BD$^\#$	BE^b
22	S	83	6(11)	BE	BF^b
23	Ş	261	1(9)9	F$^\#$DD	G^{b}EE
24	T	84	70	CF	CE$^\#$
25	U	85	71	CF$^\#$	CG^b
26	Ü	154	10(10)	D$^\#$D$^\#$	E^{b}E^b
27	V	86	72	CG	CG
28	W	87	73	CG$^\#$	CA^b
29	X	88	74	CA	CA
30	Y	89	75	CA$^\#$	CB^b
31	Z	90	76	CB	CB

Order	Character	ASCII Code	12 Base Value	Nota Sequence	Eqivalent Note
0	(space)	32	28	GC$^\#$	GD^b
1	!	33	29	GD	GD
2	#	35	2(11)	DB	DC^b
3	$	36	30	D$^\#$C	E^{b}B$^\#$
4	‘	39	33	D$^\#$D$^\#$	E^{b}E^b
5	(	40	34	D$^\#$E	E^{b}F^b
6	)	41	35	D$^\#$F	E^{b}E$^\#$
7	*	42	36	D$^\#$F$^\#$	E^{b}G^b
8	+	43	37	D$^\#$G	E^{b}G
9	,	44	38	D$^\#$G$^\#$	E^{b}A^b
10	-	45	39	D$^\#$A	E^{b}A
11	.	46	3(10)	D$^\#$A$^\#$	E^{b}B^b
12	/	47	3(11)	D$^\#$B	E^{b}C
13	:	58	4(10)	EA$^\#$	F^{b}B^b
14	<	60	50	FC	E$^\#$B$^\#$
15	=	61	51	FC$^\#$	E$^\#$D^b
16	>	62	52	FD	E$^\#$D
17	?	63	53	FD$^\#$	E$^\#$E^b
18	@	64	54	FE	E$^\#$F^b
19	[	91	77	GG	GG
20	\	92	78	GG$^\#$	GA^b
21	]	93	79	GA	GA

Order	Character	ASCII Code	12 Base Value	Nota Sequence	Equivalent Note
0	a	97	81	C$^\#$F$^\#$	D^{b}G^b
1	b	98	82	C$^\#$G	D^{b}G
2	c	99	83	C$^\#$G$^\#$	D^{b}A^b
3	ç	135	(11)3	EG$^\#$	F^{b}A^b
4	d	100	84	C$^\#$A	D^{b}A
5	e	101	85	C$^\#$A$^\#$	D^{b}B^b
6	f	102	86	C$^\#$B	D^{b}B
7	g	103	87	C$^\#$C	D^{b}C
8	ğ	259	1(9)7	F$^\#$DC	G^{b}DC
9	h	104	88	C$^\#$C$^\#$	D^{b}D^b
10	ı	213	1(5)9	F$^\#$A$^\#$D	G^{b}B^{b}D
11	i	105	89	C$^\#$D	D^{b}D
12	j	106	8(10)	C$^\#$D$^\#$	D^{b}E^b
13	k	107	8(11)	C$^\#$E	D^{b}F^b
14	l	108	90	DF	DE$^\#$
15	m	109	91	DF$^\#$	DG^b
16	n	110	92	DG	DG
17	o	111	93	DG$^\#$	DA^b
18	ö	148	1(0)4	F$^\#$FA	G^{b}FA
19	p	112	94	DA	DA
20	q	113	95	DA$^\#$	DB^b
21	r	114	96	DB	DB
22	s	115	97	DC	DC
23	ş	260	1(9)8	F$^\#$DC$^\#$	G^{b}DD^b
24	t	116	98	DC$^\#$	DD^b
25	u	117	99	DD	DD
26	ü	125	(10)5	D$^\#$A$^\#$	E^{b}B^b
27	v	118	9(10)	DD$^\#$	DE^b
28	w	119	9(11)	DE	DF^b
29	x	120	(10)0	D$^\#$F	E^{b}E$^\#$
30	y	121	(10)1	D$^\#$F$^\#$	E^{b}G^b
31	z	122	(10)2	D$^\#$G	E^{b}G

Table 13: Symbols Transmission According to F Clef

Table 15: Uppercases Transmission
Table 16: Lowercases Transmission
According According to G Clef

G Clef

Table 18: Numbers Transmission According to G Clef

Order	Character	ASCII Code	12 Base Value	Note S.	Equivalent Note
0	0	48	40	EC	$F^bB^{\#}$
1	1	49	41	$EC^{\#}$	F^bD^b
2	2	50	42	ED	F^bD
3	3	51	43	$ED^{\#}$	F^bE^b
4	4	52	44	EE	F^bF^b
5	5	53	45	EF	$F^bE^{\#}$
6	6	54	46	$EF^{\#}$	F^bG^b
7	7	55	47	EG	F^bG
8	8	56	48	$EG^{\#}$	F^bA^b
9	9	57	49	EA	F^bA

22	_	95	7(11)	GB	GC^b
23	≥	256	1(9)4	$C^{\#}AE$	D^bAF^b
24	≤	257	1(9)5	$C^{\#}AF$	$D^bAE^{\#}$

Table 17: Symbols Transmission According to G Clef

In these tables, except for some exceptional notes, the richness of the application is created by the fact that each character generally has two different representations. In our dataset, 6 characters have a single note sequence. For this reason, the number of possible representations of a text with n characters ranges from a minimum of 1 to a maximum of 2^n. Considering the key selection as well, the representation richness ranges between 3 and 3.2^n.

Example1: Let's encrypt our text "Mat .24".

Let's choose the C key as the key.

$M = F^{\#}\ F = G^b\ E^{\#}$

$a = G^{\#}\ C^{\#} = A^b\ C^{\#}$

$t = A\ G^{\#} = A\ A^b$

$. = D^{\#}\ A^{\#} = E^b\ B^b$

$2 = E\ D = E\ D$

$4 = E\ E = E\ F^b$

Mat.24 $\equiv F^{\#}FG^{\#}C^{\#}AG^{\#}D^{\#}A^{\#}EDEE$

$\equiv G^bE^{\#}A^bC^{\#}AA^bE^bB^bEDEF^b$

The expression "Mat. 24" has 16 different equivalent representations (2.2.2.1.2 = 16), which provides ease of application. Considering the clef selection, there are 48 possible representations (16 × 3 = 48).

For decryption, characters with two alternative representations are identified in our data table, allowing for easy decryption from the table.

3.2. Keyed Transmission

The key in question here is the one used in symmetric encryption.

3.2.1. Keyed Encryption Utilizing The ⊕ and ⊖ Subtraction Operations.

The $\oplus$ and $\ominus$ operations are defined in base 12.

X: Plaintext,

Y: Clef,

Z: Ciphertext

Encryption: $Z = X \oplus Y$,

Decryption: $Z \ominus Y = X$

One of the three keys is selected for the design of the dataset.

Example2 Let's encrypt our text "Mat.24".

Let's choose the C clef as the clef.

M = C C$^{\#}$

a = D$^{\#}$ G$^{\#}$

t = E D$^{\#}$

. = A$^{\#}$ F

2 = B A

4 = B B

Mat.24 ≡
As the key

Y: BG$^{\#}$C$^{\#}$EDA$^{\#}$CF$^{\#}$BA$^{\#}$

4 1 6 9 7 3 5 (11) 4 3 (10) 4

X: CC$^{\#}$D$^{\#}$G$^{\#}$ED$^{\#}$A$^{\#}$FBABB

4 1 6 9 7 3 5 (11) 4 3 (10) 4

$X \oplus Y = Z$

1 5 2 4 2 5 (10) (11) 0 (11) 6 0

Z: G$^{\#}$CABACFF$^{\#}$GF$^{\#}$C$^{\#}$G

is obtained.

3.2.2. Encrypting the Text Using Symmetric Key Operation

In this application, a key is selected for the dataset, the original notes of the characters in the dataset are taken, and a key is chosen for encryption. The text is encrypted according to the key, and for decryption, the symmetry is applied in reverse. The symmetry operation is performed in base 12.

3.2.2.1 . Date-Based Dynamic Encryption in Terms of Clef Selection

In this section, the clef selection in key-based encryption is created by converting the elements of the time component, even when encrypted, into a structure that is compatible with the note's mod12 system.

Our time component is taken as: Day-Month-Year-Hour-Minute-Second.

Example3: Let's derive the message key according to the C clef for the message sent on 12.11.2023 at 21:19:45.
$12 \equiv 0 \ (\text{mod}12) = C$
$11 \equiv 11 \ (\text{mod}12) = B$
$2023 \equiv 7 \ (\text{mod}12) = G$
$21 \equiv 9 \ (\text{mod}12) = A$
$19 \equiv 7 \ (\text{mod}12) = G$
$45 \equiv 1 \ (\text{mod}12) = C^{\#}$

Our key text would be "CBAAGC$^{\#}$".

This key selection algorithm allows for a dynamic key structure since the components of time change numerically as they are taken.

3.2.3. Dynamic Encryption Supported by Date-Composite Operations

We will define a composite operation based on musical terms such as Flat (♭) and Sharp (#).

K = {C, C$^{\#}$, D, D$^{\#}$, E, F, F$^{\#}$, G, G$^{\#}$, A, A$^{\#}$, B}

Sharp (#)

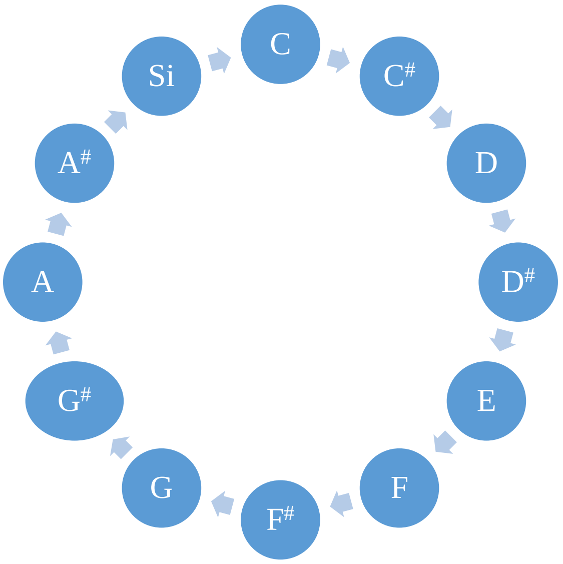

Figure 7: Sharp Composite Operation

$f: K \longrightarrow K$
$f(x): x^{\#}$

For example

$f(C): C^{\#}$
$f(C^{\#}): D$

One step clockwise.

Let's define the composite operation.

$fof(x)=(x^{\#})^{\#}$

Flat (♭)

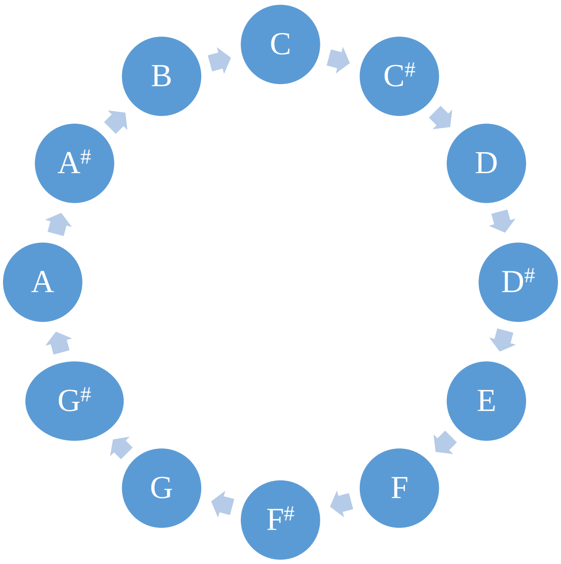

Figure 8: Flat Composite Operation

$g: K \longrightarrow K$
$G(x): x^{b}$

For example
$g(C): B^{b}$
$g(B^{b}): A^{\#}$

One step counterclockwise.

Let's define the composite operation.
$gog(x)=(x^{b})^{b}$

Let's define another composite operation.
$gof(x)=(x^{b})^{\#}$

f and g are inverse operations of each other.

We will use the Day-Month data as the time unit.
Let our time be represented as **ab cd**.

The function **f** will be associated with the day, and the function **g** will be associated with the month.

The composite function choices for the characters were selected based on the order of the characters in the text.

Character Order/ Unit Used	Solo	Duo
Composite Operation	f	g

Table 19: Matching of Function-Date

Example3: Let's send the expression **Mat.24** = $F^{\#}FG^{\#}C^{\#}AG^{\#}D^{\#}A^{\#}$EDEE on 03.09.

M: The composition operation is applied three times with the f function, $F^{\#}F$.

fofof($Fa^{\#}$) = (($Fa^{\#})^{\#})^{\#}$ = La
fofof(Fa) = (($Fa^{\#})^{\#})^{\#}$ = $Sol^{\#}$

a: The composition operation is applied nine times with the g function, $G^{\#}C^{\#}$.

gogog...og($Sol^{\#}$) = Si
gogog...og($Do^{\#}$) = Mi

If the operations continue similarly, ...

Character	Note Sequence	Order	Function	Operations Number	New Note Sequence
M	$F^{\#}F$	1	f	3	A $G^{\#}$
A	$G^{\#}C^{\#}$	2	g	9	B E
T	A $G^{\#}$	3	f	3	C B
.	$D^{\#}$ $A^{\#}$	4	g	9	$G^{b}D^{b}$
2	E D	5	f	3	G F
4	E E	6	g	9	G G

Table 20: The Encryption of the Mat.24 Text According to the Above Data

We obtain,

Mat.24 = $AG^{\#}$ $BECBG^{b}D^{b}GFGG$

For the decryption process, only f and g are applied in reverse. That is, if the sequence number is odd, the g function is used, and if it is even, the f function is used, and if necessary, it is converted to the equivalent note.

3.2.4. Date-Music Key-Composition Operation Supported Dynamic Encryption

In this section, the integer part of the time will be taken.

Date: Day-Month-Hour

Music Key: C, G, F

Composition Operation: f and g

Day: Gives the number of compositions of the f function.

Month: Gives the number of compositions of the f function.

Hour: Affects the selection of the key.
(C: hour = 0 (mod 3))
(F: hour = 0 (mod 3))
(G: hour = 1 (mod 3))

Composition Function:
If the character's sequence number is odd, use the f function;
If the character's sequence number is even, use the g function.

Example: Let's send the Mat.24 message on 02.03 at 19:00.

The composition count of the function f is 2. The composition count of the function g is 3.

Clef: G, 19≡1 (mod 3) thus we obtain Mat.24 = $CC^{\#}D^{\#}G^{\#}ED^{\#}A^{\#}FBABB$

Character	Note Sequence	Order	Function	Operition Number	New Note Sequence
M	$C\ C^{\#}$	1	f	2	$D\ D^{\#}$
A	$D^{\#}G^{\#}$	2	g	3	C F
T	$E\ D^{\#}$	3	f	2	$D\ C^{\#}$
.	$A^{\#}F$	4	g	3	G D
2	F B	5	f	2	$G\ C^{\#}$
4	B B	6	g	3	$G\ C^{\#}$

Table 21: The Encryption of the Mat.24 Text According to the Above Data

Encrypted text is $DD^{\#}CFDC^{\#}GDGC^{\#}GC^{\#}$.

If the elements in the odd rows are composed twice with g, and the elements in the even rows are composed three times, the original text will be restored.

3.2.5. Data Character Transformation in Terms of Note-Keyed Dynamic Hybrid Encryption

In this algorithm, while the original text is being encrypted, a hybrid music key structure is created. Our primary variable will be the sequence number of the element to be encrypted within the text.

For sequence number: n, the clefs...

C hour ≡ 0 (mod 3)
G hour ≡ 1 (mod 3)
F hour ≡ 0 (mod 3)
are determined as follows.

Example:
Let's encrypt Mat.24.

M and . = C
a and 2 = G
t and 4 = F

3.2.6. Key, Flat, and Sharp Sign-Based Encryption on the Musical Staff

In this section, encryption will be performed using the clef, flat (♭), and sharp (♯) signs on the musical staff. The key to be used at the beginning of the musical staff and the flat and sharp signs for the notes will be marked. Let's design an encryption system based on these markings. Let’s design a cyclical system based on the sequence number.

Clef:
Transformation of the data set

#: Odd-numbered components
♭: Even-numbered components

If neither the flat (♭) nor the sharp (#) sign is present, the corresponding elements remain unchanged.

Example4:
Let the musical staff have the C key and sharp (#).
Let’s encrypt Mat.24.

Mat.24 ≡ $F^{\#}$ F $G^{\#}$ $C^{\#}$ A $G^{\#}$ $D^{\#}$ $A^{\#}$ E D E E
Since only the sharp (#) sign is used, when the odd-numbered components are shifted by the sharp,

Mat.24 ≡ G F A $C^{\#}$ $A^{\#}$ $G^{\#}$ E $A^{\#}$ F D F E
will be the encrypted form.

4.CONCLUSİON AND DISCUSSION

In this study, a 12-note system based on the 7-note Pythagorean diatonic scale has been modeled, which is adapted to Turkish music with support for sharps and flats. The system was analyzed through three different musical keys, resulting in three distinct representations of the dataset and equivalent note notations. The transformation methods between the musical keys were derived and formulated.

Symmetric encryption with text-based keys was modeled in two versions in terms of the encryption process. Additionally, three original versions of dynamic encryption were developed, incorporating time-based aspects. In the dynamic encryption involving historical and composite operations, an innovative algorithm was developed, particularly focused on operations involving sharps and flats.

For data character transformation, an original dynamic hybrid encryption was developed, taking into account the character's sequence number and the musical key. Furthermore, a novel encryption algorithm was created based on the musical staff and associated hardware.

In conclusion, the modeling of the 12-note system of Turkish makam music with three different keys and the representation of each character through equivalent musical notes introduces an innovative and original algorithm to the literature. Our algorithm, with its modular arithmetic, addition, subtraction, symmetry, and composite function designs, is unique in its construction. The algorithm is further strengthened by its complexity, incorporating time and sequence number concepts, the composite function, encryption key, and hybrid encryption using three keys. The use of frequency analysis and the reduction of similarity between terms in ASCII code structure result in a cipher that is resistant to decryption.

Acknowledgments

The author declares that there is no conflict of interest. The authors have contributed equally to this study. No additional support, beyond what is covered in the author contributions and funding sections, has been received for this study.

5.REFERENCES

[1]Agahyev, M. (2017). *Kriptoloji ve veri şifreleme teknikleri üzerine* [Master's thesis, Ege University]. İzmir, Turkey.

[2]Akar, A., & Aksoy, P. (2022). *Kriptolojinin müzik dili* [TÜBİTAK 2204 Project Archive].

[3]Bakım, S. (2014). *Examination of the use of the Fibonacci sequence and the golden ratio in music* [Master's thesis, Selçuk University]. Konya, Turkey.

[4]Denizkuşu, A. (2023). *Denk notalarla şifreleme* [TÜBİTAK 2204 Project Archive].

[5]Dutta, S., Kumar, C., & Chakraborty, S. (2010). A novel method for hiding message using musical notes. *International Journal of Computer Applications, 1*(16), 76-79.

[6]Karaçam, C., Algül, F. N., & Tavit, D. (2021). Transmission of time and position variable cryptology in Fibonacci and Lucas number series with music. *Journal of Mathematical Sciences and Modelling, 4*(1), 38-50. https://doi.org/10.5430/jmsm.v4n1p38

[7]Krishnan, R., Thomas, R., Akshay, D. S., & Krishna, V. S. (2021). An intelligent text encryption system using musical notes. *Lecture Notes on Data Engineering and Communications Technologies, 59*, 449-459.

[8]Kundu, T. (2020). An approach to musical cryptography. In *Proceedings of the International Web Conference on Smart Engineering Technologies*.